AFRL-OSR-VA-TR-2013-0207

Qualitative and Quantitative Proofs of Security Properties

Joseph Halpern
Cornell University

April 2013
Final Report

AIR FORCE RESEARCH LABORATORY
AF OFFICE OF SCIENTIFIC RESEARCH (AFOSR)
ARLINGTON, VIRGINIA 22203
AIR FORCE MATERIEL COMMAND

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
22/02/2012	Final Report	

4. TITLE AND SUBTITLE
Qualitative and Qunatitivae Proofs of Security Properties

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-09-1-0226

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Joseph Halpern

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Cornell University
Sponsored Financial Services
P. O. Box 22
Ithca, NY 14851

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Office of Sponsored Research
875 N. Randolph St.
Arlington, VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)
AFOSR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The goal of this project has been to develop logics for reasoning about scurity at both the qualitative and quantitative level. Two approaches have been considered. The first builds on a logic designed by the PI that has a binary operator ->, where p->q is interested as "the probability of p given q goes to 1." The logic has been applied to proving the correctness of a variety of security protocols. Doing this required extending the original logic to include additional operators for reasoning about traces, essentially with freatures in the spirit of dynamic logic. A sound proof system for hte extended logic was devleoped. The seond approach involves a logic for reasoning about knowledge, probability and itme. A special case, restricting to only probability 1 statements, gives a qualitative logic of belief. A key innovation in the logic is distinguishing between strings and message terms. This allows an agent receiving a string s that represents a message m encrypted by a key k to be uncertain about what message term the string s represents. It is shown that this approach deals with resource-bounded agents in a natural and powerful way.

15. SUBJECT TERMS
Cryptography, probability, security, quantitative, qualitative, conditional logic, knowledge, strings, messages.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Joseph Halpern
unclassified	unclassified	unclassified	UU	7	19b. TELEPHONE NUMBER *(Include area code)* 607-255-9562

Qualitative and Quantitative Proofs of Security Properties: Final Report

Joseph Y. Halpern

Grant No: AFOSR FA9550-09-1-0266
PI: Joseph Y. Halpern
Institution: Cornell University, Ithaca, NY 14853

Goals and Accomplishments

Two largely disjoint approaches have been used to prove the correctness of security protocols. The first essentially ignores the details of cryptography by assuming perfect cryptography (i.e., nothing encrypted can ever be decrypted without the encryption key) and an adversary that controls the network. By ignoring the cryptography, it is possible to give a more qualitative proof of correctness, using logics designed for reasoning about security protocols. Indeed, this approach has enabled axiomatic proofs of correctness and model checking of proofs. The second approach applies the tools of modern cryptography to proving correctness, using more quantitative arguments. Typically it is shown that, given some security parameter k (where k may be, for example, the length of the key used) an adversary whose running time is polynomial in k has a negligible probability of breaking the security, where "negligible" means "less than any inverse polynomial function of k."

The goal of this project has been to develop logics for reasoning about security at both the qualitative and quantitative level. Two approaches have been considered. The first builds on a logic designed by the PI that has a binary operator $\rightarrow$, where $\phi \rightarrow \psi$ is interpreted as "the probability of ψ given ψ goes to 1." Proof of qualitative statements of the form $\phi \rightarrow \psi$ in the logic can automatically be converted to proofs of quantitative statements of the form $\phi \rightarrow^r \psi$, where r is a real number in $[0, 1]$, which is interpreted as "the probability of ψ given ϕ is at least $1 - r$." In joint work with Anupam Datta, John Mitchell, and Arnab Roy, the logic has been applied to proving the correctness of a variety of security protocols. Doing this required extending the original logic to include additional operators for reasoning about traces, essentially with features in the spirit of dynamic logic. A proof system for the extended logic was developed that was shown to be rich enough to prove correctness of a variety of protocols. Interactions between the conditional probability assertions and dynamic logic assertions were studied.

The second approach, joint work with the PI, Ron van der Meyden, and Riccardo Pucella, involves a logic for reasoning about knowledge, probability, and time. A special case, restricting to only probability 1 statements, gives a qualitative logic of belief. By allowing arbitrary probability statements, more quantitative statements can be expressed. A key innovation in

the logic is distinguishing *strings* from *messages* as a way to capture the fact that agents are resource bounded. For example, suppose that i sends j the message $\mathbf{m}'$, where $\mathbf{m}'$ is $\mathbf{m}$ encrypted by a shared key k. Does j know that i has sent $\mathbf{m}$ encrypted by k? If j does not have the key k, then, intuitively, the answer is no; agent j has no way of knowing that $\mathbf{m}'$ is the result encrypting $\mathbf{m}$ by k. Of course, if j were not computationally bounded, then j could figure out that $\mathbf{m}'$ is indeed $\mathbf{m}$ encrypted by k. Standard approaches to modeling knowledge treat agents as computationally unbounded; in particular, they are assumed to know all valid formulas. Since the fact that $\mathbf{m}'$ is the result of encrypting $\mathbf{m}$ by k is a valid mathematical statement, all agents will know it.

To get around this problem, two views of messages are considered. The first views a message simply as a string of symbols; the second views the message as a term with structure. When j receives the message $\mathbf{m}'$, j knows that he received (the string) $\mathbf{m}'$. What j does not know is that he received $\mathbf{m}$ encrypted by k; j considers it possible that $\mathbf{m}'$ is $\mathbf{m}''$ encrypted by k'', or that $\mathbf{m}'$ is not the encryption of any message. By considering both strings and terms, and mappings between them, an agent can be uncertain about what term a string represents. Thus, for example, an agent i may know that `s` represents the encryption of some message, even though i does not know which message it is the encryption of. This approach deals with resource-bounded agents in a natural and powerful way.

Personnel Supported

Danny Dolev (senior visitor); Joseph Halpern (PI); Vasumathi Raman (Ph.D. student); Nan Rong (Ph.D. student); Lior Seeman (Ph.D. student); Dongcai Shen (M.Sc. student)

Publications supported by grant (April 1, 2009 - Nov. 30, 2012)

Journal publications

1. J. Y. Halpern and S. Petride, A knowledge-based analysis of global function computation, *Distributed Computing* **23**:3, 2010, pp. 197–224.

2. M. Bickford, R. L. Constable, J. Y. Halpern, and S. Petride, Knowledge-based synthesis of distributed systems using event structures, *Logical Methods in Computer Science* **7**:2, 2011.

3. I. A. Kash, E. J. Friedman, and J. Y. Halpern, Multiagent learning in large anonymous games, *Journal of AI Research* **40**, 2011, pp. 571–598.

4. L. C. Rêgo and J. Y. Halpern, Generalized solution concepts in games with possibly unaware players, *International Journal of Game Theory* **41**:1, 2012, pp. 131–155.

5. I. A. Kash, E. J. Friedman, and J. Y. Halpern Optimizing scrip systems: Crashes, altruists, hoarders, sybils and collusion, *Distributed Computing*, 2011.

6. P. D. Grünwald and J. Y. Halpern, Making decisions using sets of probabilities: updating, time consistency, and calibration, *Journal of AI Research* **42**, 2011, pp. 393-426.

7. J. Y. Halpern and with R. Pucella, Modeling adversaries in a logic for security protocol analysis, *Logical Methods in Computer Science* **8**:1, 2012.

8. J. Y. Halpern and R. Pass, Iterated regret minimization: a new solution concept, *Games and Economic Behavior* **74**:1, 2012, pp. 194–207.

9. J. Y. Halpern and L. C. Rêgo, Reasoning about knowledge of unawareness revisited, to appear, *Mathematical Social Sciences*.

10. J. Y. Halpern and L. C. Rêgo, Extensive games with possibly unaware players, to appear, *Mathematical Social Sciences*.

11. J. Y. Halpern and C. Hitchcock, Compact representations of extended causal models, to appear, *Cognitive Science*.

12. J. Y. Halpern, From causal models to counterfactual structures, to appear, *Review of Symbolic Logic*.

Conference publications

13. D. J. Martin, J. Gehrke, and J. Y. Halpern, Shared winner determination in sponsored search auctions *Proceedings of the 25th International Conference on Data Engineering*, 2009, pp. 270–280.

14. I. A. Kash, E. J. Friedman, and J. Y. Halpern Multiagent learning in large anonymous games, *Proceedings of the Eighth International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, 2009, pp. 765–772.

15. I. A. Kash, E. J. Friedman, and J. Y. Halpern Manipulating scrip systems: sybils and collusion, *Proceedings of the First Conference on Auctions, Market Mechanisms, and Multiagent Systems (AMMA)*, 2009.

16. J. Y. Halpern and R. Pass, Iterated regret minimization: A more realistic solution concept, *Proceedings of the 21st International Joint Conference on Artificial Intelligence (IJCAI 2009)*, 2009, pp. 153–158.

17. J. Y. Halpern and R. Pass, A logical characterization of iterated admissibility, *Proceedings of Twelfth Conference on Theoretical Aspects of Rationality and Knowledge (TARK)*, 2009, pp. 146–155.

18. J. Y. Halpern, R. Pass, and V. Raman, An epistemic characterization of zero knowledge, *Proceedings of the Twelfth Conference on Theoretical Aspects of Rationality and Knowledge (TARK)*, 2009, pp. 156–165.

19. J. Y. Halpern and L. C. Rêgo, Reasoning about knowledge of unawareness revisited, *Proceedings of Twelfth Conference on Theoretical Aspects of Rationality and Knowledge (TARK)*, 2009, pp. 166-173.

20. J. Y. Halpern and R. Pass, Game theory with costly computation: formulation and application to protocol security, *First Symposium on Innovations in Computer Science*, 2010, pp. 120–142

21. J. Y. Halpern and N. Rong, Cooperative equilibrium, *Proceedings of the Ninth International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS 2010)*, 2010, pp. 1465-1466

22. J. Y. Halpern, From causal models to counterfactual structures, *Proceedings of the Twelfth International Conference on Principles of Knowledge Representation and Reasoning (KR 2010)*, 2010, pp. 153–160.

23. J. Y. Halpern and R. Pass, I don't want to think about it now: Decision theory with costly computation, *Proceedings of the Twelfth International Conference on Principles of Knowledge Representation and Reasoning (KR 2010)*, 2010, pp. 182–190.

24. J. Y. Halpern, N. Rong, and A. Saxena, MDPs with Unawareness, *Proceedings of the Twenty-Sixth Conference on Uncertainty in AI (UAI 2010)*, 2010, pp. 228–235.

25. A. Bjorndahl, J. Y. Halpern, and R. Pass, Reasoning about justified belief, *Proceedings of Thirteenth Conference on Theoretical Aspects of Rationality and Knowledge (TARK)*, 2011, pp. 221–227.

26. D. Dolev, D. Feitelson, J. Y. Halpern, R. Kupferman, and N. Linial, No justified complaints: on fair sharing of multiple resources, *Proceedings of 3rd Conference on Innovations in Theoretical Computer Science (ITCS 2012)*, 2012.

27. J. Y. Halpern and W. Kets, Ambiguous language and differences in beliefs, *Proceedings of the Thirteenth International Conference on Principles of Knowledge Representation and Reasoning (KR 2012)*, 2012, pp. 329–338.

28. J. Y. Halpern, R. Pass, and L. Seeman, I'm doing as well as I can: modeling people as rational finite automata, *Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence (AAAI-12)*, 2012, pp. 1917-1923.

29. J. Y. Halpern and S. Leung, Weighted sets of probabilities and minimax weighted expected regret: new approaches for representing uncertainty and making decisions, *Proceedings of the Twenty-Seventh Conference on Uncertainty in AI (UAI '2012)*, pp. 336-345.

30. A. Bjorndahl, J. Y. Halpern, and R. Pass, Language-based games, *Proceedings of Fourteenth Conference on Theoretical Aspects of Rationality and Knowledge (TARK)*, 2013, pp. 39-48.

31. J. Y. Halpern and R. Pass, Game theory with translucent players, *Proceedings of Fourteenth Conference on Theoretical Aspects of Rationality and Knowledge (TARK)*, 2013, pp. 216-221.

32. J. Y. Halpern and N. Rong, Towards a deeper understanding of cooperative equilibrium: characterization and complexity, *Proceedings of the Twelfth International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS 2013)*, 2013.

Major invited presentations (April 1, 2009 - Nov. 30, 2012):

- Beyond Nash equilibrium: solution concepts for the 21st century,
  - GAMES Summer School, Bertinoro, Italy (June, 2009)
  - Behavioral and Quantitative Game Theory: Conference on Future Directions, Newport Beach, California (May, 2010)
  - HEC, Paris, France (January 2011)
  - Saul Gorn Memorial Lecture, U. Pennsylvania, Philadelphia, Pennsylvania (April 2011)
  - Tenth International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS), Taipei, Taiwan (May, 2011)
  - Twelfth Computing in the 21st Century Conference, Beijing, China (October 2011)
  - GAMESEC (Conference on Decision Theory and Game Theory for Security), College Park, Maryland (Nov., 2011)
  - C3E (Computational Cybersecurity in Compromised Environments), West Point, New York (Sept., 2012)
  - Turing Centenary Celebration, Melbourne, Australia (Dec., 2012).
- Game Theory with Costly Computation
  - Sackler Lecture, Tel Aviv University Economics Dept, Tel Aviv, Israel (October 2009)
  - Champery Spring School, Champery, Switzerland (Feb., 2010)
- Iterated Regret Minimization: A New Solution Concept
  - Center for Rationality, Hebrew University, Jerusalem, Israel (Jan. 2010)
  - Champery Spring School, Champery, Switzerland, Feb., 2010
- Defaults and normality in causal structures,
  - MICRAC Workshop on Causality in AI and Cognitive Psychoology Toulouse, France (June 2009)
- Distributed Computing Meets Game Theory: Robust Mechanisms for Secret Sharing and Implementation with Cheap Talk
  - Technion (January, 2010)
  - Champery Spring School, Champery, Switzerland (Feb., 2010)
- Knowledge and common knowledge in multi-agent systems
  - Fulbright Distinguished Lecture, Hebrew University (March, 2010)
- Intransitivity and Vagueness

  - 31st Linz Seminar on Fuzzy Set Theory, Linz, Austra, February 2010

- Constructive Decision Theory
  - LSE, London, England (January 2011)
  - 11th European Conference on Symbolic and Quantitative Approaches to Reasoning with Uncertainty, Belfast, Ireland (June 2011)
  - Games 2012, Naples, Italy (September 2012)
  - Australasian Joint Conference on Artifical Intelligence (December 2012).
- Causality, Responsibility, and Blame
  - Conference on Scalable Uncertainty Management (SUM 2011), Dayton, Ohio (Oct. 2011)
  - Lisbon Workshop on Causality and Inference, Lisbon, Portugal (May 2012)
- Reasoning about Knowledge of Awareness Revisited
  - Workshop on Unawareness: Conceptualization and Modelling, Johns Hopkins, Baltimore, Maryland (October, 2011)
- Sequential Equilibrium in Games of Imperfect Recall
  - Workshop on Extensive Form Games in Honor of Harold Kuhn, Vienna, Austria (June 2012)
- Robustness and Optimization of Scrip Systems
  - CWI, Amsterdam, Netherlands (January, 2011)
  - Google Tech Talk, Google, New York City, NY (December 2012)
- Awareness in Games, Awareness in Logic,
  - LPAR-17 (Seventeenth International Conference on Logic for Programming, Artificial Intelligence, and Reasoning), Yogyakarta, Indonesia (Oct., 2010).

Consultative and advisory functions

None.

New discoveries, inventions or patent disclosures

None.

Honors/Awards
(All awards in this reporting period; major awards from earlier periods)

- "Language-based games" selected as one of two top papers from TARK (Conference on Theoretical Aspects of Reasoning About Knowledge) to be presented at session at IJCAI 2013 on best papers from related conferences.
- "Ambiguous language and differences in beliefs" given the Ray Reiter Best Paper award at the Thirteenth International Conference on Knowledge Representation and Reasoning, 2012.
- Selected IEEE Fellow, 2012
- Selected Economic Theory Fellow, Society for the Advancement of Economic Theory, 2011
- ACM SIGART Autonomous Agents Research Award, 2011
- Saul Gorn Memorial Lecturer, University of Pennsylvania, 2011.
- Fulbright Distinguished Chair in Natural Sciences and Engineering, Hebrew University, 2009-10
- Kenneth A. Goldman '71 Excellence in Teaching Award, 2010
- Sackler Lecturer, Tel Aviv University, 2009
- 2009 Edsger Dijkstra Prize in Distributed Computing
- 2008 ACM/AAAI Newell Award
- Selected Fellow of AAAS, November, 2005.
- Selected Fellow of ACM, 2002.
- Awarded 1997 Gödel Prize for outstanding paper in the area of theoretical computer science for "Knowledge and common knowledge in a distributed environment".
- Fellow of the American Association of Artificial Intelligence, 1993.